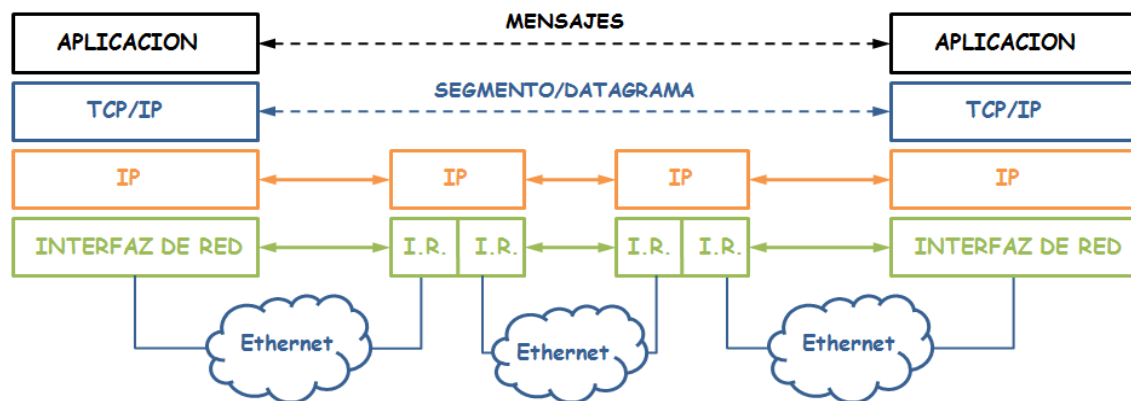


# TEMA 2: NIVEL DE RED TCP/IP.

## 1. INTRODUCCIÓN.



- **NIVEL IP:** Fundamentado en los routers, pone en común las comunicaciones e independiza las tecnologías subyacentes.

Crea un esquema de direccionamiento común para que la información llegue a cualquier maquina del mundo.

- **DIRECCIONAMIENTO IP:** Son 4 octetos separados por puntos, es decir, 32 bits que se agrupan en grupos de 8 bits (1 byte)

Los octetos se expresan en decimal.

DIRECCION RED	DIRECCION MAQUINA
---------------	-------------------

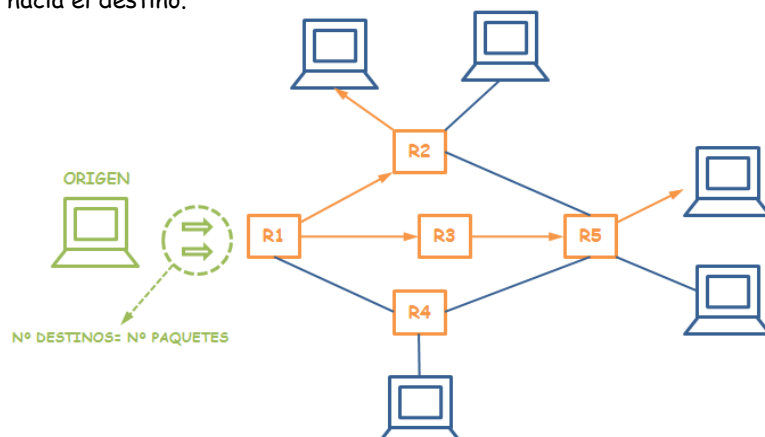
- **DIRECCION DE RED:** Organiza por redes generales independientemente de la maquina destino.  
Dos equipos conectados a la misma red tienen la misma dirección de red.
- **DIRECCION DE MAQUINA:** Identifica el equipo dentro de la red. Cada usuario se identifica con una dirección IP diferente.

Se encamina hacia redes, no hacia equipos.

## 2. ENVIO DE PAQUETE IP.

- **UNIDIFUSION:** Por cada paquete IP que envías lo tienes que replicar por el número de destinos a los que van dirigidos.

Simplifica el encaminamiento, dices a donde quieres que vaya cada paquete (cada equipo tiene su propia IP) y los routers se encargan de encaminar hacia el destino.





- **PROBLEMA:** Se está replicando la información de forma innecesaria cuando lo único que cambia es la IP destino.  
Proceso de envío independiente desde una maquina origen a una única maquina destino.

- **MULTIDIFUSION:** Con una misma dirección IP podemos acceder a muchos equipos (los que tenga asignada la dirección).

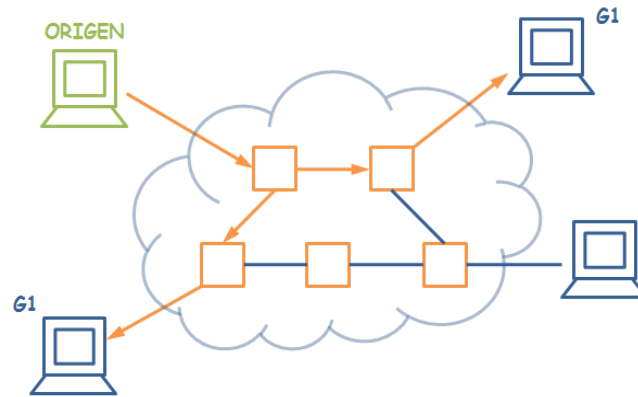
Además de su IP cada equipo puede asimilar otras direcciones IP para conectar vía multicast.

- **ROUTERS MULTICAST:** Tiene tablas de rutas especiales para multicast.

Localiza los equipos con dirección IP multicast, copia el paquete IP y lo encamina hacia los equipos.

Desde la maquina origen solo sale un único paquete IP, son los routers los que lo copian para encaminar a los distintos equipos con mismo grupo multicast.

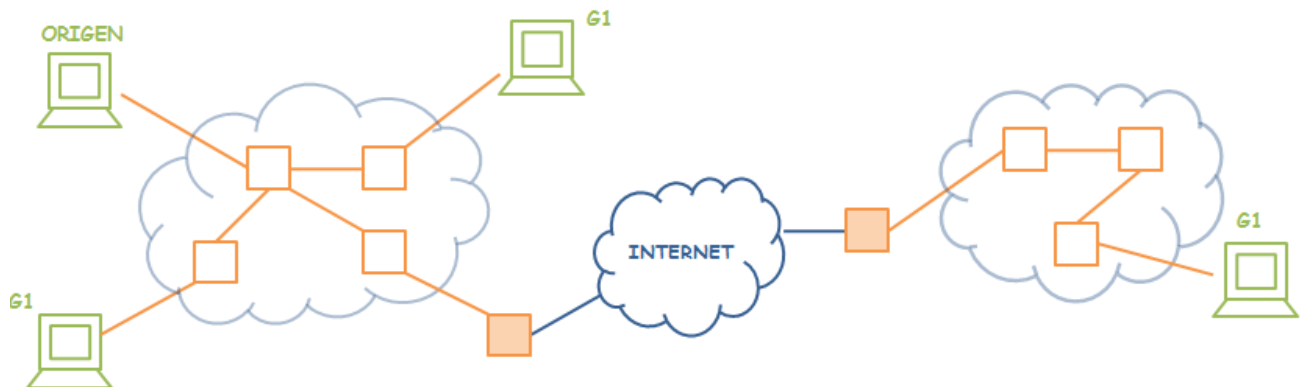
Muy complicada la fiabilidad.



Multidifusión consiste en un único proceso de envío independientemente del número de maquinas receptoras.

- **ARBOL MULTIDIFUSION:** Grafo con todos los caminos.

No se puede hacer multicast en internet pero si en una red local.



Es imposible que multicast funcione en internet porque cuando llega un paquete multicast a internet esta se descarta.

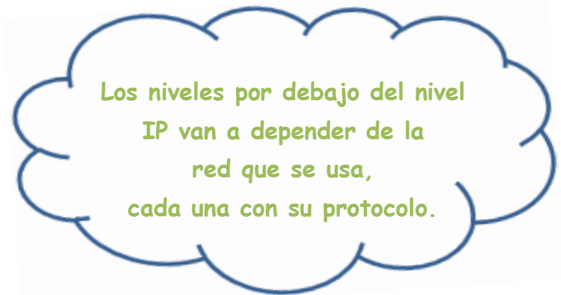
Para poder hacerlo se usa M-Bone. Suscriben los routers que encaminen a la red donde está el equipo de multicast y solo hay que indicar que en la red que conecta con el router esta G1 (destino).

Para ello se encapsula el protocolo, es decir, el paquete IP con la información de introduce dentro de otro paquete IP que contendrá como dirección destino el router.

Cuando un paquete IP no es tratable en Internet se encapsula dentro de otro paquete IP con un destino que si es tratable en internet.



En este caso el nivel IP tendrá que trabajar el doble: tratar el paquete IP externo y el del paquete que se envía con el destino multicast.



- **DIFUSION:** Broadcast

El paquete va dirigido a todos los equipos de la red. Solo se envía un datagrama (datagrama IP de difusión) independientemente del número de máquinas receptoras.

Restringido a redes locales.

### 3. DIRECCIONES IP.

Las direcciones IP se pueden dividir en cinco bloques, teniendo en cuenta los tres tipos de transmisión IP y los bits para identificar las redes.

La división en bloques nos permite encaminar de forma eficiente.

Los 32 bits de la dirección IP nos permitirían tener  $2^{32}$  direcciones IP distintas, pero sería inviable direccionarlas si son independientes, por tanto, se organizan en bloques o clases.

- **CLASE A:**

Tamaño del bloque = 1/2 Tamaño Bloque total ( $2^{32}$ )



Son redes escasas pero muy grandes lo que hace que sean las más caras.

- **FORMATO:** RED. MAQUINA.MAQUINA.MAQUINA

El rango teórico de direcciones de red van de 0.0.0.0 - 127.0.0.0 pero el rango práctico va de la dirección 1.0.0.0 - 126.0.0.0

El rango completo de direcciones para este tipo de redes será: 1.0.0.0 - 126.255.255.254

- **CLASE B:**

Tamaño de la clase B es la mitad del tamaño de la clase A, es decir, un 1/4 Tamaño Bloque total ( $2^{32}$ )



Tenemos más redes disponibles pero son de menor tamaño.

- **FORMATO:** RED. RED.MAQUINA.MAQUINA

El rango de direcciones de red van desde 128.0.0.0 - 191.255.0.0

El rango completo de direcciones para este tipo de redes será: 128.0.0.0 - 191.255.255.254

- **CLASE C:**

Tamaño de la clase C es la mitad del tamaño de la clase B, es decir, un 1/8 Tamaño Bloque total ( $2^{32}$ )

Son redes que usan pequeñas y medianas empresas.



Tenemos disponibles muchísimas redes pero de tamaño muy pequeño.

- **FORMATO:** RED. RED.RED.MAQUINA

Las redes que se agrupan en las clases A, B o C son redes de unicast o unidifusión.



- **CLASE D:** Son redes de multidifusión. No se usan mucho.



- **CLASE E:** Redes reservadas para un formato futuro o experimental. Son redes perdidas ( $2^{28}$  redes) ya que no se pueden utilizar.



### 3.1 DIRECCIONES RESERVADAS.

- **REDES:** Solo influye a las redes de clase A.

- **0.0.0.0:** Ruta por omisión.

Ruta a la que encaminan los routers cuando no saben a dónde encaminar.

- **127.0.0.0:** Dirección de red bucle o LOOPBACK.

Se usa para pruebas de procesos servidores y en el desarrollo de aplicaciones TCP/IP de cliente-servidor.

Se usa en aplicación en red dentro de la propia máquina.

- **DIR MAQUINA:** Incluye a las clases A, B y C.

- **RED.0.0.0 /RED.RED.0.0 /RED.RED.RED.0:** Hacen referencia a la dirección de red.

Ruta a la que encaminan los routers cuando no saben a dónde encaminar.

- **RED.255.255.255 /RED.RED.255.255 /RED.RED.RED.255:** Broadcast dirigido (local)

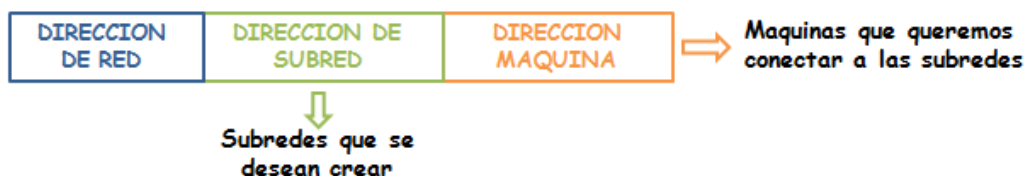
Difusión dirigida a subredes Ethernet, se pone a unos la parte de bits dedicados a equipos, es decir, el paquete se manda a todos los equipos que pertenezcan a la red sobre la que se hace broadcast.

- **255.255.255.255:** Broadcast limitado.

Se manda el paquete a todas las máquinas que pertenezcan a la misma red que la máquina que envía el paquete.

## 4. SUBREDES.

Redes propias que crea un administrador a partir de la dirección IP oficial asignada a su organización y crear localmente sus propias direcciones IP.



Los criterios a tener en cuenta para crear subredes son:

1. La clase de la dirección IP asignada oficialmente.
2. Numero de subredes que se desean crear y numero de máquinas que se desean conectar dichas subredes.
3. Direcciones reservadas (dirección de red y broadcast).

Cada vez que se crea una subred (como potencia de dos), lo más seguro es perder direcciones además de las que están ya reservadas.

- **RESTRICCIONES DE LA RFC:**

- **TODO 0'S:** No se podría usar porque se confundiría con la dirección IP de la red oficial.

Solo se podrían distinguir por los bits de la máscara asociada.

- **TODO 1'S:** Nos confundiríamos con la dirección de broadcast dirigido de la red asociada a IP oficial.

Como el broadcast dirigido no se usa y la dirección con la parte de equipos a cero la podemos identificar con su máscara vamos a obviar la RFC y las vamos a usar.



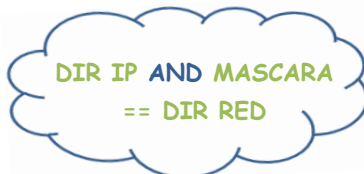
## 4.1 MASCARAS.

Una máscara de red es un número de 32 bits que contiene 1's en los bits que identifican a la red.

Una dirección IP lo único que te dice es de qué clase es la red con la que vamos a trabajar, pero no te dice si pertenece a una subred y ha cual, por tanto tenemos que aplicar una máscara.

Para generar una máscara tenemos que localizar donde está la división de subred  $\Rightarrow$  vamos a poner a 0 la parte de equipos y el resto a 1.

Un router lo que hace es aplicar máscaras para saber a dónde encaminar, va a realizar una AND.

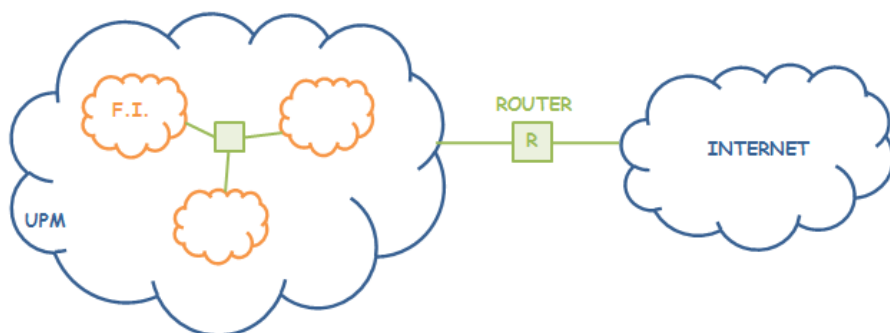


• **MÁSCARA POR OMISION:** Se utiliza cuando nos dan una dirección y no nos dan la máscara que lleva asociada. Es la máscara de la red global.

- **CLASE A:** 255.0.0.0
- **CLASE B:** 255.255.0.0
- **CLASE C:** 255.255.255.0

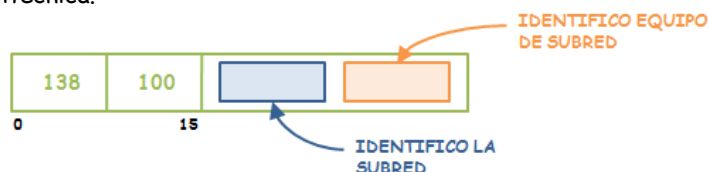
Las máscaras no tienen nada que ver con la clase de una red. Podemos tener una red de clase B que tenga dos subredes y que su máscara sea la misma que la máscara global de una red de clase C.

\* **EJEMPLO  $\Rightarrow$**  Sea la dirección 138.100.0.0, la dirección de red que identifica a la red de la UPM (red de clase B) y la dirección de la red de la facultad de informática es 138.100.8.0



Desde internet solo se sabe que se va a tener que ir encaminando al router R.

Se va a dividir la red UPM en varias subredes que identifican las distintas universidades que pertenecen a la politécnica.



Como la UPM tiene 26 centros, vamos a necesitar 26 subredes. Como  $2^4=16$  no tenemos suficientes  $\Rightarrow 26 < 2^5=32$  vamos a necesitar 5 bits.

1 0 0 0 0 1  
0 0 0 1 0

26 1 1 0 1 0

1 1 1 1 0

$\Rightarrow$  Perdemos  $32 - 26 = 2 \times 2^{16-5}$  debido a la organización interna en subredes.

Podríamos añadir hasta 6 centros sin tener que modificar la estructura creada o incluso hasta 8 centros si no consideramos la RFC.



Si consideramos que a la red de la FI se compone de los siguientes equipos:

138.100.9.34 y 138.100.9.0



No indica subred, sino 8 bits (solo 5 indican la subred, los otros 3 son de equipo).

Vamos a calcular a que red pertenecen, para ello aplico una máscara:

```
138.100.9.34 = 138. 100. 0 0 0 0 1 0 0 1. 0 0 1 0 0 0 1 0
255.255.1 1 1 1 1 0 0 0. 0 0 0 0 0 0 0 0
-----
138. 100. 0 0 0 0 1 0 0 0. 0 0 0 0 0 0 0 0 ⇒ 138.100.8.0
```

Los valores de las máscaras van a cambiar según el número de subredes, la máscara asociada a la subred 138.100.8.0 es la 255.255.248.0.

Dada la dirección de subred 138.100.8.0 la dirección de broadcast dirigida a la subred será 138.100.15.255.

138.100. 0 0 0 0 1 1 1 1. 1 1 1 1 1 1 1 1 ⇒ DIRECCION EQUIPOS A 1'S

Del mismo modo la dirección de broadcast dirigida a toda la red de la UPM será 138.100.255.255

Una máscara se puede expresar con el numero explicito, expresado en octetos o diciendo el numero de 1's que tiene máscara.

#### • CLASES DE MÁSCARAS:

- **LONGITUD FIJA:** Solo permiten una misma mascara a las subredes creadas. Se asigna una misma cantidad máxima de maquinas, es decir, todas las redes son del mismo tamaño.
- **LONGITUD VARIABLE:** Permiten aplicar diferentes máscaras a las subredes creadas. Asignamos cantidades variables de maquinas, es decir, el tamaño de las redes va a depender del número de equipos que vayan a tener.

## 5. ENCAMINAMIENTO

#### • TIPOS DE ENCAMINAMIENTO:

- **DIRECTO:** El router sabe a qué red hay que enviar porque el router conecta a ambas (Una única interfaz de salida).
- **INDIRECTO:** Entre las redes origen y destino hay varios routers entre medias y vamos a tener que ir encaminando al router que más nos acerque al equipo destino (interfaz de salida de la red).
- **POR OMISION:** 0.0.0.0  
Se usa para encaminar por internet  
Se pone siempre la última en la tabla de rutas

#### • MASCARAS Y ENCAMINAMIENTO:

- **0'S:** El bit correspondiente en la dirección IP de destino no es significativa a la hora de encaminar, ya que se encamina hacia redes, no hacia maquinas.
- **1'S:** El bit correspondiente en la dirección IP de destino es muy significativo para la función de encaminamiento, ya que hace referencia a la parte de la red de la dirección.

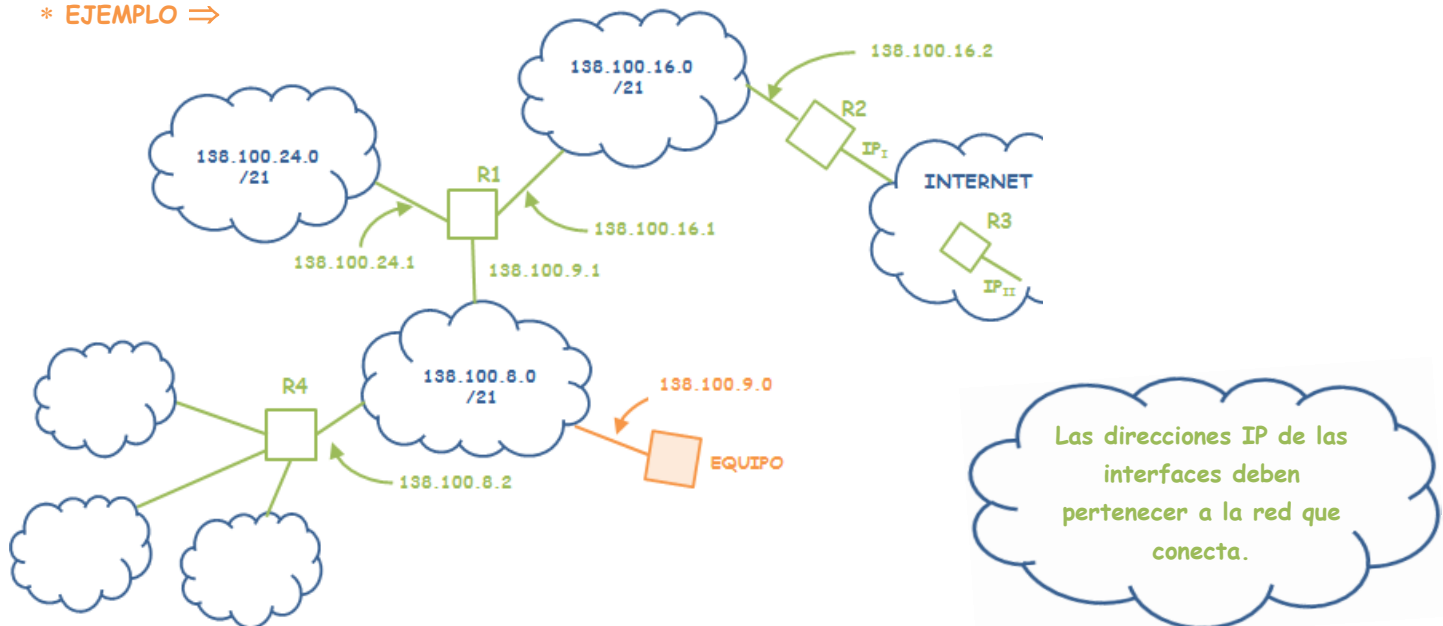


## 5.1 TABLAS DE RUTAS PARA MASCARAS FIJAS.

Tenemos que tener en cuenta que no se pueden solapar direcciones y que los routers deben tener una visión general.

Las tablas de rutas dependen del sistema operativo que estemos usando. Las entradas más prioritarias van primero en la tabla por que se van leyendo de forma secuencial.

\* EJEMPLO ⇒



- ROUTER R1:

DIRECCION DE RED	MASCARA	INTERFAZ DE SALIDA	DESTINO
138.100.16.0	/21	138.100.16.1	Directo
138.100.8.0	/21	138.100.9.1	Directo
138.100.24.0	/21	138.100.24.1	Directo
0.0.0.0	/0	138.100.16.1	138.100.16.2

- ROUTER R2: Siguiendo el mismo procedimiento que con el router anterior

DIRECCION DE RED	MASCARA	INTERFAZ DE SALIDA	DESTINO
138.100.16.0	/21	138.100.16.2	Directo
138.100.8.0	/21	138.100.16.2	138.100.16.1
138.100.24.0	/21	138.100.16.2	138.100.16.1
0.0.0.0	/0	IP <sub>I</sub>	IP <sub>II</sub>

Esta tabla no es optima, lo mejor es agrupar las redes que no son de acceso directo, por tanto vamos a encaminar a la red principal, donde se incluyen el resto de las subredes y será el router R1 en el que mire las subredes. Tenemos que reducir la máscara porque si no estaríamos mirando las subredes y no la red principal.

DIRECCION DE RED	MASCARA	INTERFAZ DE SALIDA	DESTINO
138.100.16.0	/21	138.100.16.2	Directo
<b>138.100.0.0</b>	<b>/21</b>	<b>138.100.16.2</b>	<b>138.100.16.1</b>
0.0.0.0	/0	IP <sub>I</sub>	IP <sub>II</sub>

Agrupar es muy cuando tenemos muchos niveles de redes, pero puede producir rebotes entre routers. Para evitar rebotes (a pesar del time to live) añadimos una entrada en el router R1 para que toda red que pertenece a la red 138.100.0.0 que no aparezca en la tabla se descarte.

Esta entrada se debe añadir antes de la entrada por omisión.



DIRECCION DE RED	MASCARA	INTERFAZ DE SALIDA	DESTINO
138.100.16.0	/21	138.100.16.1	Directo
138.100.8.0	/21	138.100.9.1	Directo
138.100.24.0	/21	138.100.24.1	Directo
<b>138.100.0.0</b>	<b>/16</b>	<b>127.0.0.1</b>	<b>127.0.0.1</b>
0.0.0.0	/0	138.100.16.1	138.100.16.2

Si tuviésemos en cuenta la subred conectada por el router R4 en vez de descartar el resto de redes debemos añadir una nueva entrada en la tabla de rutas del router R1.

DIRECCION DE RED	MASCARA	INTERFAZ DE SALIDA	DESTINO
138.100.16.0	/21	138.100.16.1	Directo
138.100.8.0	/21	138.100.9.1	Directo
138.100.24.0	/21	138.100.24.1	Directo
<b>138.100.0.0</b>	<b>/16</b>	<b>138.100.9.1</b>	<b>138.100.8.2</b>
0.0.0.0	/0	138.100.16.1	138.100.16.2

El descarte (si es necesario) se hará en las tablas de rutas del router R4

- **EQUIPO:** Tendrá que decidir si encamina a la red con la que se conecta de forma directa o a los distintos routers que conectan con otras redes (R1 o R4), por tanto hay que buscar la forma más eficiente de agrupar, es decir, jugaremos con las máscaras.

Suponemos: 138.100.16.0 = 138.100.0 0 0 0 0 0 1 0.0  
 138.100.24.0 = 138.100.0 0 0 1 1 1 0 0.0  
 138.100.0 0 0 1 1 1 0 0.0  
 138.100.0 0 0 1 1 0 0 0.0  
 138.100.0 0 0 1 0 1 0 0.0

} Ambas redes se encaminan por R1

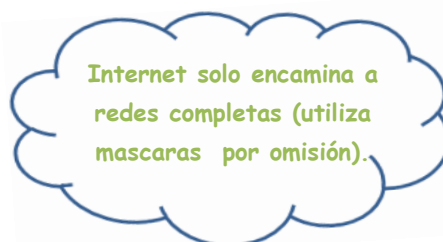
} Las redes se encaminan por R4

Vamos a usar las mascarar que nos permitan agrupar pero también nos permitan distinguir las redes dentro del grupo.

DIRECCION DE RED	MASCARA	INTERFAZ DE SALIDA	DESTINO
138.100.8.0	/21	138.100.9.0	Directo
138.100.0.0	/19	138.100.9.1	138.100.9.1
138.100.0.0	/16	138.100.9.0	138.100.8.2
0.0.0.0	/0	138.100.9.0	138.100.9.1

Las mascara que se ponen en tablas de rutas pueden ser la de la propia red (se encaminan a todas las redes por separadas) o se puede usar una máscara menor que agrupe algunas redes ⇒ MASCARA TRUCO. (Solo encamina al grupo de redes)

Si este criterio se aplica a redes completas (A,B,C) los grupos se denominan superred.



- **TIME\_TO\_LIVE:** Contador que va en la cabecera IP del paquete que indica cuantas veces se puede encaminar el paquete antes de descartarse.



## 5.2 TABLAS DE RUTAS PARA MASCARAS VARIABLES.

Suponemos una red de clase B cualquiera (138.100.0.0 /16) dividida en varias subredes, una de ellas es 138.100.64.0 /18. Queremos que esta subred se divida en otras subredes más pequeñas, pero no tienen el mismo tamaño.

SBR1: 136 Equipos

SBR2: 329 Equipos

SBR3: 500 Equipos

SBR4: 2000 Equipos

Podemos:

1. Como tenemos cuatro subredes, solo vamos a necesitar 2 bits (si no seguimos la RFC)

/20 ← .....  
138.100.0100:0000.0  
          01  
          10  
          11

En este caso todas las subredes son del mismo tamaño, es decir, tenemos  $2^{8+6}$  equipos disponibles para trabajar (hacer mas subredes o poner equipos)

Solo hay que hacer la máscara lo más grande posible y que asignar todas las subredes necesarias, peor no es ampliable

2. Damos el mínimo tamaño posible de red y luego si fuese necesario ampliarla, aumentando el número de redes o incluso aumentando el número de equipos.

Por tanto:

SBR1: 136 Equipos  $\Rightarrow 2^8$

SBR2: 329 Equipos  $\Rightarrow 2^9$

SBR3: 500 Equipos  $\Rightarrow 2^9$

SBR4: 2000 Equipos  $\Rightarrow 2^{11}$

Lo que vamos a hacer es poner la cifra de los equipo en potencia de dos ( $2^x$ ) donde x son los bits necesarios para direccionar los equipos.

Vamos a jugar con las mascarar ya que son las que determinan el tamaño de una red.

138.100.0100:0000.0  $\Rightarrow$  138.100.64.0 /24  
          000:010:0  $\Rightarrow$  138.100.66.0 /23  
          000:100:0  $\Rightarrow$  138.100.70.0 /23  
          001:110:0  $\Rightarrow$  138.100.72.0 /21  
          /21 /23 /24



Tenemos que poder distinguir entre mascarar (como mínimo en 1 bit). Lo mejor es cambiar los bits de menor peso para poder añadir más redes posteriormente.

La máscara de una red distingue su red del resto.

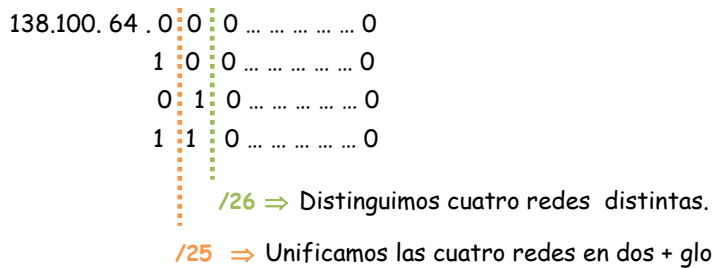
- **OBTENER MASCARAS:** Cuando no nos dan el número de equipos de manera explícita para nosotros obtengamos las mascarar vamos a seguir los siguientes pasos:
  1. Ordenamos las direcciones de menor a mayor
  2. Cogemos la dirección mayor y se compara con el resto de direcciones.
  3. Vamos buscando de izquierda a derecha (en la dirección IP mayor) el primer bit diferenciador que distinga a la dirección IP mayor del resto, en ese punto corta la máscara.
- **JUEGO CON SUBREDES:** Además de las redes anteriores podemos tener otras posibilidades:
  - **CON MASCARA /24:** Podemos direccionar 2 redes sin que hayan conflictos con las demás redes:
    1. 138.100.64.0 /24
    2. 138.100.65.0 /24  $\Rightarrow$  138.100.01000001.0
  - **CON MASCARA /23:** Podemos tener tres redes distintas que no dan problemas.
    1. 138.100.66.0 /23
    2. 138.100.68.0 /23  $\Rightarrow$  138.100.01000100.0
    3. 138.100.70.0 /23
  - **CON MASCARA /21:** Podemos tener  $2^3-1$  posibilidades distintas, pero hay que excluir la opción 000.



Para reducir el tamaño de una red lo único que hay que hacer es reducir el tamaño de la máscara. Por ejemplo si utilizamos una máscara /26 vamos a reducir el número de equipos de la red a 64 equipos.

Hay que ser previsor a la hora de crear las redes por si en algún momento queremos unificar, subdividir o ampliar alguna red.

- **UNIFICAR:** Reduzco la máscara  $\Leftrightarrow$  Dividir la red por la mitad



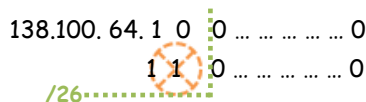
Si quisiéramos volver a la situación inicial no le influye la forma en que se gestionan las subredes.

- **SUBDIVIDIR:** Aumentamos la máscara, pero el problema está en que también hay que modificar las direcciones IP de las direcciones afectadas por el cambio de la máscara.

En el caso anterior las combinaciones 00 y 01 /25 no son validas porque no se distinguen las redes, para poder distinguirlas deberíamos utilizar máscara /26.

Si volvemos a un punto intermedio sí que hay que tener en cuenta la combinación de bits. Con máscara /25 y combinación 00 y 01 seguiríamos teniendo dos redes en vez de una como queremos, lo correcto sería utilizar la máscara /26.

- **CRECER:** Si queremos que en un futuro una red pueda crecer, es decir, unificarla tenemos que tener cuidado de no usar combinaciones consecutivas.



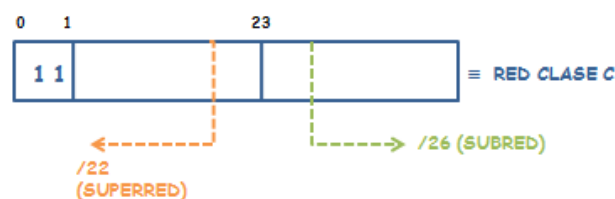
La combinación 11 no es viable porque cuando unifique se van a juntar en una sola red y no es eso lo que quiero. Lo que haría es utilizar 01 y dejar 11 para ampliar con máscara /25 cuando sea necesario.



## 6. SUPERREDES

- **SUPERRED:** Nos permiten agrupar varias redes y encaminar solo hacia una única entrada en la tabla ahorrándonos entradas en la tabla de rutas.

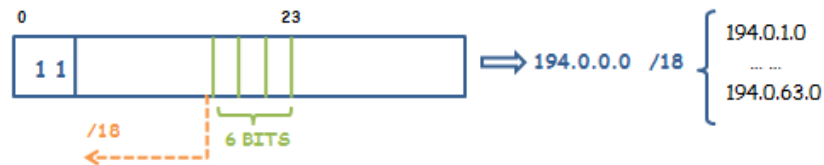
Se usan en redes de clase C, para evitar dar redes de clase B a lo loco y así evitar que se consuman todas.



Usamos combinaciones de 2 bits  $\Rightarrow$  4 superredes de clase C pero esto no siempre se puede hacer porque a lo mejor invadimos otra red de clase C ya asignada.



- \* **EJEMPLO**  $\Rightarrow$  Queremos 33 redes de clase C para una organización. Como con 5 bits solo podemos crear 32 superredes vamos a necesitar 6 bits (64 redes)



Cuando queramos encaminar a cualquier de estas redes solo tenemos que encaminar hacia la dirección 194.0.0.0 /18. Para crear superredes podemos utilizar todos los bits excepto los 2 primeros que identifican el tipo de red.

Si ahora necesitamos otras 32 redes  $\Rightarrow$  no necesitamos consumir otros 5 bits solo haría falta mover la máscara y añadir un 1, así ya diferenciamos ambas superredes.

194.0.01:000000.0  $\Rightarrow$  194.0.64.0 /19  
/19

Bits para definir subredes dentro de la red

Si luego quisiéramos otras 32 redes podríamos usar la combinación 11, en caso de necesitar más redes tendríamos que volver a añadir un bit más y modificar la máscara o bien unificar en el primer caso no nos quedaría hueco.

Cuando la mascar es menor que /24 estamos hablando de superred; si es mayor generamos subredes de una red de clase C.

Unificando todo:

/18  $\leftarrow$  194.0.00000000.0  $\Rightarrow$  194.0.0.0 /18  
...  
00111111.0  $\Rightarrow$  194.0.63.0 /18  
-----  
194.0.01000000.0  $\Rightarrow$  194.0.64.0 /19  
...  
010111111.0  $\Rightarrow$  194.0.95.0 /19  
/19  $\leftarrow$

¡¡NO  
TOCAR!!!

La combinación 01 no se puede usar por que la superred anterior ya la usa. Por tanto si queremos dar 33 redes podríamos usar una subred de 32 redes y una sola red aparte, en vez de dar una única superred de 64 redes y perder 31 redes.

En vez de dar la potencia de 2 mayor al nº de redes solicitado, vamos a dar 1 asuma de redes potencias de dos que más se acerca a la pedida  $\Rightarrow$  SOLO SUPERREDES!!, NUNCA SUBREDES!!

## 7. DIRECCIONAMIENTO PRIVADO

Hay ciertas direcciones de red que no se pueden usar para encaminar por internet  $\Rightarrow$  **REDES PRIVADAS**

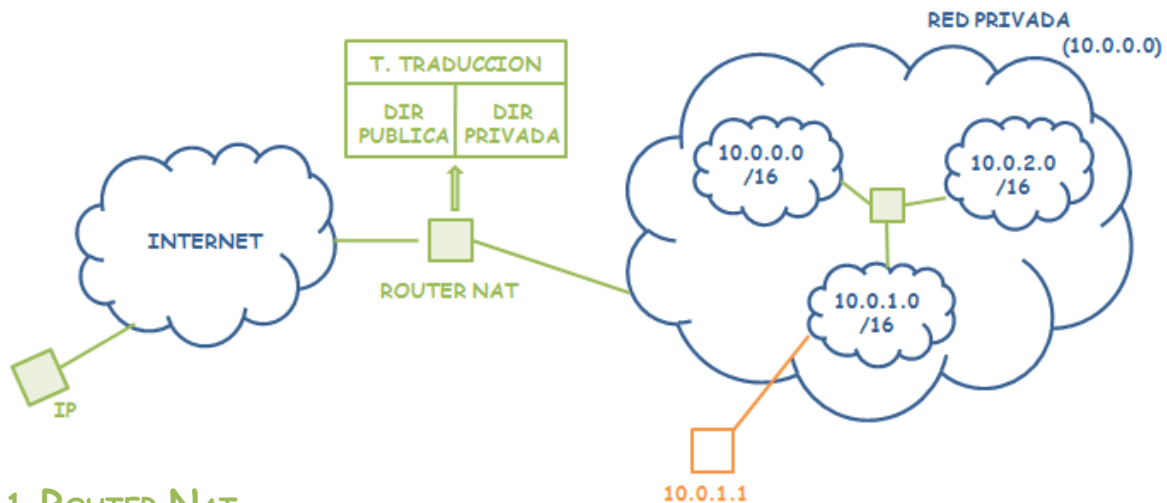
- **OBJETIVO:** No agotar las direcciones IP publicas asignables y para que no pueda acceder directamente a internet.

Las redes privadas son:

- \* 10.0.0.0  $\Rightarrow$  1 red de clase A (10.0.0.0 - 10.255.255.255)
- \* 172.16.0.0 - 172.31.0.0  $\Rightarrow$  16 redes contiguas de clase B
- \* 192.168.0.0  $\Rightarrow$  1 red de clase C (256 direcciones)



Se opera igual que con otra red encaminable por internet.



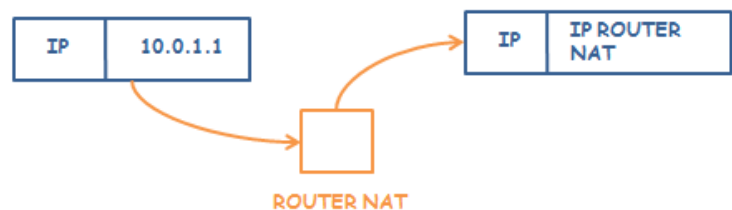
## 7.1 ROUTER NAT.

Trabaja a nivel IP realizando traducciones entre direcciones IP privadas y las direcciones IP públicas (oficiales).

Si queremos mandar un paquete no tenemos problemas, los problemas aparecen cuando se quiere recibir un paquete desde internet.

El router NAT usa una tabla de traducciones NAT donde guarda la dirección privada y su traducción a red pública para que al enviar desde internet el router sepa hacia donde encaminar.

\* **EJEMPLO** ⇒ Enviamos paquete desde 10.0.1.1 hacia IP.



El router NAT cambia la IP origen (10.0.01) por la IP del router NAT y se guarda en la tabla de traducciones. Para volver lo único que tiene hacer el router es acceder a la tabla de traducciones y volver a cambiar la dirección IP destino (IP router NAT) por la del equipo de la red privada (10.0.1.1).

### • TIPOS DE ROUTERS NAT:

#### - POR MODO DE FUNCIONAMIENTO:

- \* **NAT UNIDIRECCIONAL (NAT BASICO)** ⇒ Comunicaciones unidireccionales salientes para clientes internos.
- \* **NAT BIDIRECCIONAL** ⇒ Comunicaciones bidireccionales para ofrecer al exterior servidores internos.

#### - POR MODO DE TRADUCCION:

- \* **NAT ESTATICO** ⇒ Número de direcciones publicas igual al de direcciones privadas.
- \* **NAT DINAMICO** ⇒ Traducción automatizada y temporal. Reutilización de direcciones.

#### - POR NIVEL DE COMUNICACIONES:

- \* **NAT BASICO** ⇒ Nivel IP.
- \* **PNAT** ⇒ Nivel IP y nivel de transporte (numero de puerto).

Con una dirección pública se pueden representar hasta 65.535 maquinas privadas asociando estática o dinámicamente de dirección IP privada y el nº de puerto privado con una dirección IP pública y un puerto libre.



## 7.2 ROUTER PNAT.

Permite que con una única dirección pública se puedan conectar más de una red privada a la vez.

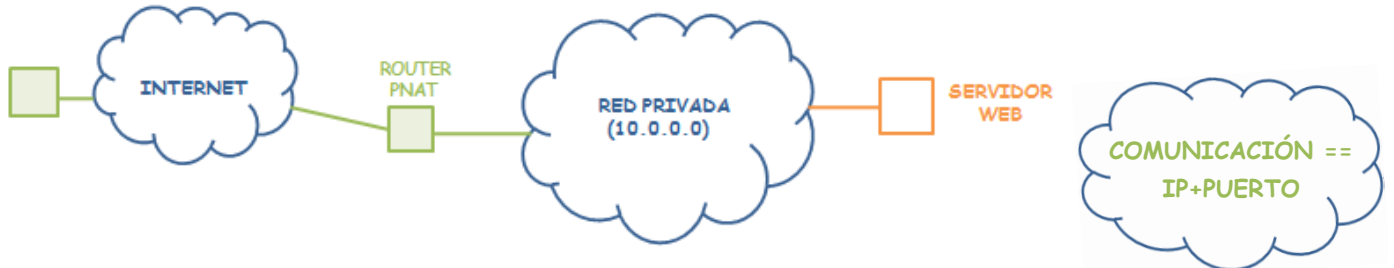
El router tiene que traducir la IP privada y el número de puerto privada a una IP pública y un puerto libre (superior a 1024).

Se usa para servidores Web

Se usa tabla PNAT de traducciones  $\Rightarrow$

IP_PRIV: PUERTO_PRIV	IP_PUBL: PUERTO_PUBL
----------------------	----------------------

Cuando tenemos varias conexiones a la vez lo único que hay que hacer es poner distinto número de puerto libre.

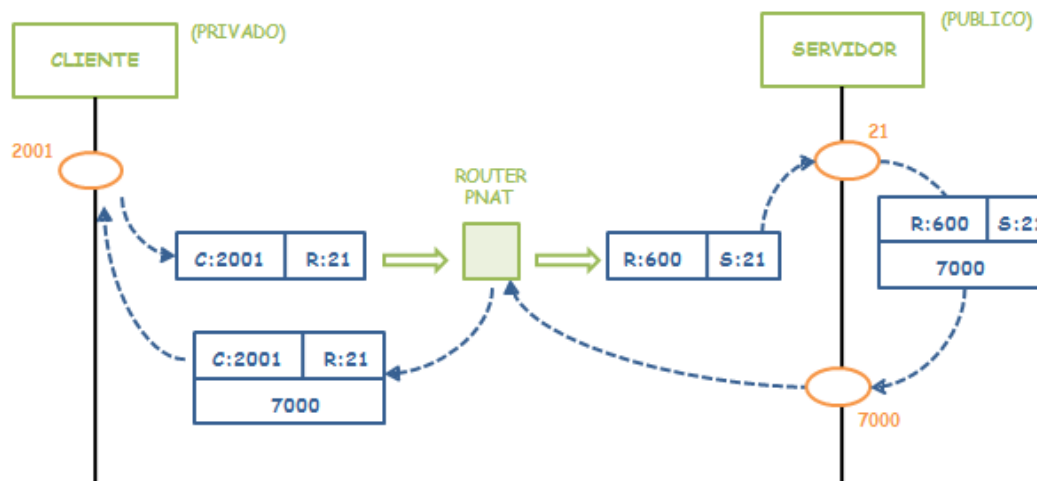


Si ahora quisiéramos conectar un servidor Web a la red privada (Puerto 80):

- \* El router PNAT conoce la IP del servidor y se marca que el puerto 80 se asocia a la IP del servidor.
- \* Para enviar al servidor lo único que hay que hacer es indicar el puerto y olvidarnos de la IP.

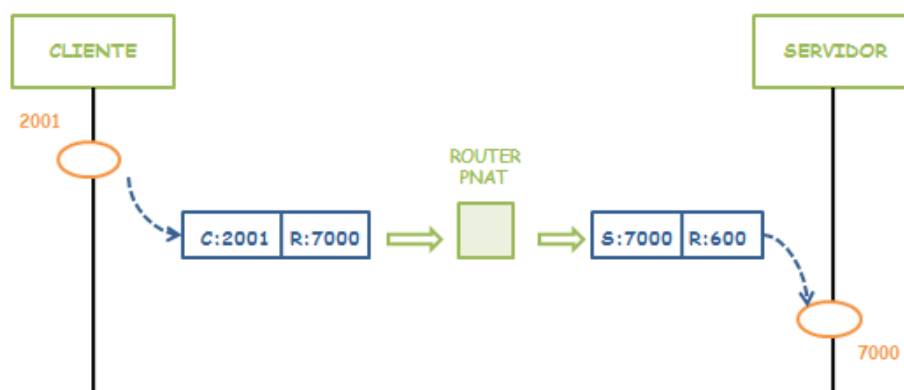
Si quisiéramos 2 IP distintas para el puerto 80 vamos a necesitar dos IP públicas para asignar el puerto 80 2 veces, es decir, dos entradas en la tabla PNAT

\* **EJEMPLO  $\Rightarrow$  SERVIDOR FTP PÚBLICO Y CLIENTE FTP PRIVADO.**



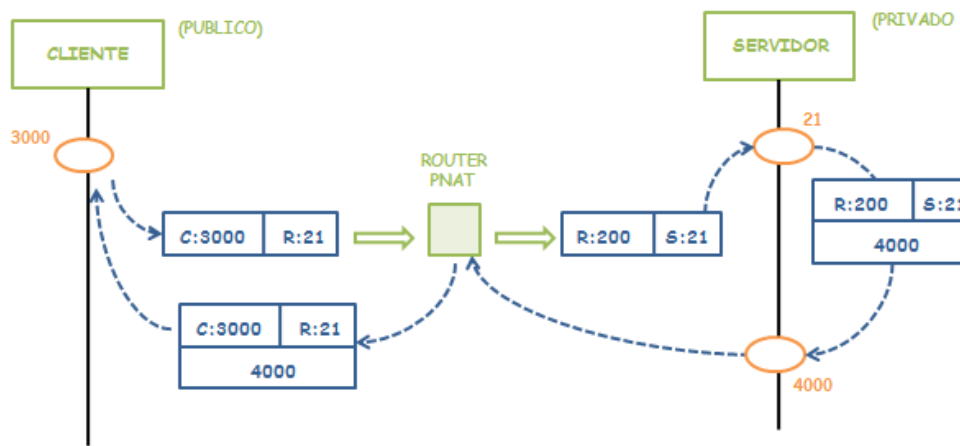
El servidor TCP recibe todas las solicitudes de conexión en un mismo puerto (21) y luego abre un puerto concreto para realizar cada comunicación.

Como el servidor es público el router PNAT sabe acceder al puerto concreto (7000) y comenzar la comunicación con ese puerto.





\* **EJEMPLO** ⇒ SERVIDOR FTP PRIVADO Y CLIENTE FTP PÚBLICO.



Cuando se quiere comenzar la comunicación FTP el router no tiene en su tabla que IP está asociada al puerto 4000 y por tanto va a fallar.

Para solucionarlo el router PNAT necesita conocer el protocolo de aplicación FTP, es decir, tiene que saber cómo funciona el servicio FTP

Vamos a añadir otra nueva entrada en la tabla de traducciones del router PNAT tal que una misma IP (S) tiene dos puertos asociados.

## 8. PROTOCOLO IPV4.

El protocolo IPV4 es el protocolo actual de encaminamiento TCP/IP mediante un servicio no orientado a conexión. Ofrece la posibilidad de encaminamiento-fragmentación.

No hay control de errores no control de flujo, solo detecta los errores físicos en la cabecera IP.

• **PROTOCOLO IPV6:** Protocolo futuro de encaminamiento TCP/IP mediante un servicio no orientado a conexión.

Es una adaptación del protocolo IPV4 para incrementar el espacio de direcciones IP a 16 octetos, agilizar el encaminamiento, la transmisión de audio y video en tiempo real y para transmisiones seguras.

### 8.1 DATAGRAMA IPV4.

Un datagrama se compone de una cabecera IP y de los datos. Como mínimo la cabecera IP va a ser 20 octetos.

El tamaño del datagrama IP no puede superar la MTU de la red, es decir, el tamaño máximo de la trama de la red. Para poder enviar un datagrama IP de tamaño mayor que la MTU de la red se necesita fragmentación.

• **FORMATO DEL DATAGRAMA IPV4:** Longitud total Max 65.535 octetos



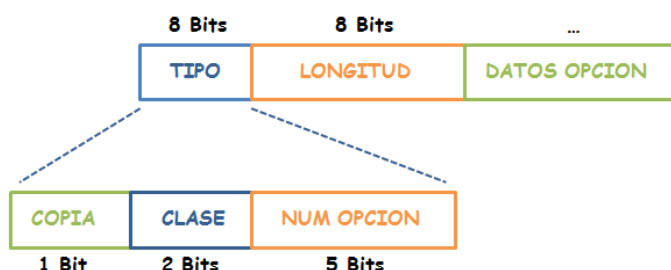
• **FRAGMENTACION:** Dividimos el paquete IP en varios fragmentos (paquetes IP independientes) que se recuperan en el origen.

### 8.2 CABECERA IP.

4 Bits	4 Bits	8 Bits	16 Bits
VERSION	Longitud Cabecera	TIPO DE SERVICIO 000 R C F 00	LONGITUD TOTAL
IDENTIFICADOR		0	D F M F DESPLAZAMIENTO
TIME TO LIVE (TTL)		PROTOCOLO	SUMA COMPROBACION (XOR) DE CABECERA
DIRECCION DE ORIGEN			
DIRECCION DE DESTINO			
OPCIONES		RELLENO	
DATOS			



- **LONGITUD CABECERA:** Numero de bloques de 4 octetos, cada bloque, del que consta la cabecera.
- **TIPO DE SERVICIO:** Consta de tres grupos:
  - **R:** Bit de mínimo retardo de transito = Normal\_Bajo.  
Se usa en telnet
  - **C:** Bit de máximo caudal retardo de transito = Normal\_Alto.  
Enviar el paquete con el mayor ancho de banda posible (Ftp)
  - **F:** Bit de mínimo fiabilidad = Normal\_Alto.  
No implica que un protocolo sea fiable.
 Para los bits C, R, F se va a solicitar lo máximo que el router puede ofrecer.
- **LONGITUD TOTAL:** Se mide en octetos, representa el tamaño de los datos y de la cabecera.  
Longitud total máxima será 65.535 octetos = 1 1 1 ....1 1.
- **IDENTIFICADOR:** Cada paquete que se envía lleva un número de identificación (contador)  
Cuando el contador llega al valor máximo, vuelve a empezar desde cero.  
El fragmento de un paquete tienen el mismo ID que el paquete original, para que el router destino los localice y los vuelva a unir.
- **DF (DENIED FRAGMENT):** Deniega la fragmentación de paquetes.  
Si un paquete no cabe dentro de la trama de la red, el paquete se desecha.  
Los paquetes cifrados o firmados no se pueden fragmentar, porque se los carga.
  - **FIRMAR UN PAQUETE:** Pone una marca a los campos que no se pueden modificar y en el destino se comprueba.
- **MF (MORE FRAGMENT):** Indica si quedan más fragmentos de un paquete.  
Todos los fragmentos tendrán MF =1 excepto el ultimo que lo tiene a MF =0.
- **DESPLAZAMIENTO:** Numero de bloques de 8 octetos contenido en el campo de datos en fragmentos anteriores.  
Indica cuantos bloques van antes del fragmento que estamos enviando.  
Si DF=1  $\Rightarrow$  Desplazamiento = 0.  
MF =1 + Desplazamiento  $\Rightarrow$  permite al router destino recomponer los fragmentos.
- **TIME TO LIVE (TTL):** Número máximo de saltos que puede dar un paquete antes de ser descartado.  
Número máximo = 255.  
Con cada encaminamiento el contador se decrementa y cuando llega a cero se elimina. Cuando un paquete llega al destino y en ese último salto el TTL ha pasado a ser cero el paquete no se va a descartar.
- **PROTOCOLO:** Identifica el SAP o el protocolo del nivel superior.  
Cada protocolo tiene número asociado: TCP =6, UDP=17, ICMP=1, IP=4.
- **SUMA DE COMPROBACION:** Chequea si la cabecera es correcta.
- **OPCIONES:** Campo de información de control (longitud variable) para servicios adicionales.



- **COPIA:**
  - \* **COPIA=1:** El campo opción se debe copiar en todos los fragmentos.
  - \* **COPIA=0:** El campo opción se copia solo en el primer fragmento.
- **CLASE =0 =CONTROL:**
  - \* **SEGURIDAD:** nivel de confidencialidad
  - \* **ENCAMINAMIENTO DESDE EL ORIGEN:** estricto o no estricto.



\* REGISTRO RUTA: Identificar IP de cada router.

\* SELLO DE TIEMPO: Identificación del momento en que un router procesa un datagrama.

### 8.3 FRAGMENTACION.

Se produce cuando introducimos una información que es mayor que el tamaño de la trama de la red, lo que se va a hacer es dividir el paquete en fragmentos.

• **MTU:** Tamaño de la trama de la red. Incluye el tamaño de la cabecera y el tamaño de los datos.

MTU por omisión  $\Rightarrow$  1500 octetos (Ethernet y PPP).

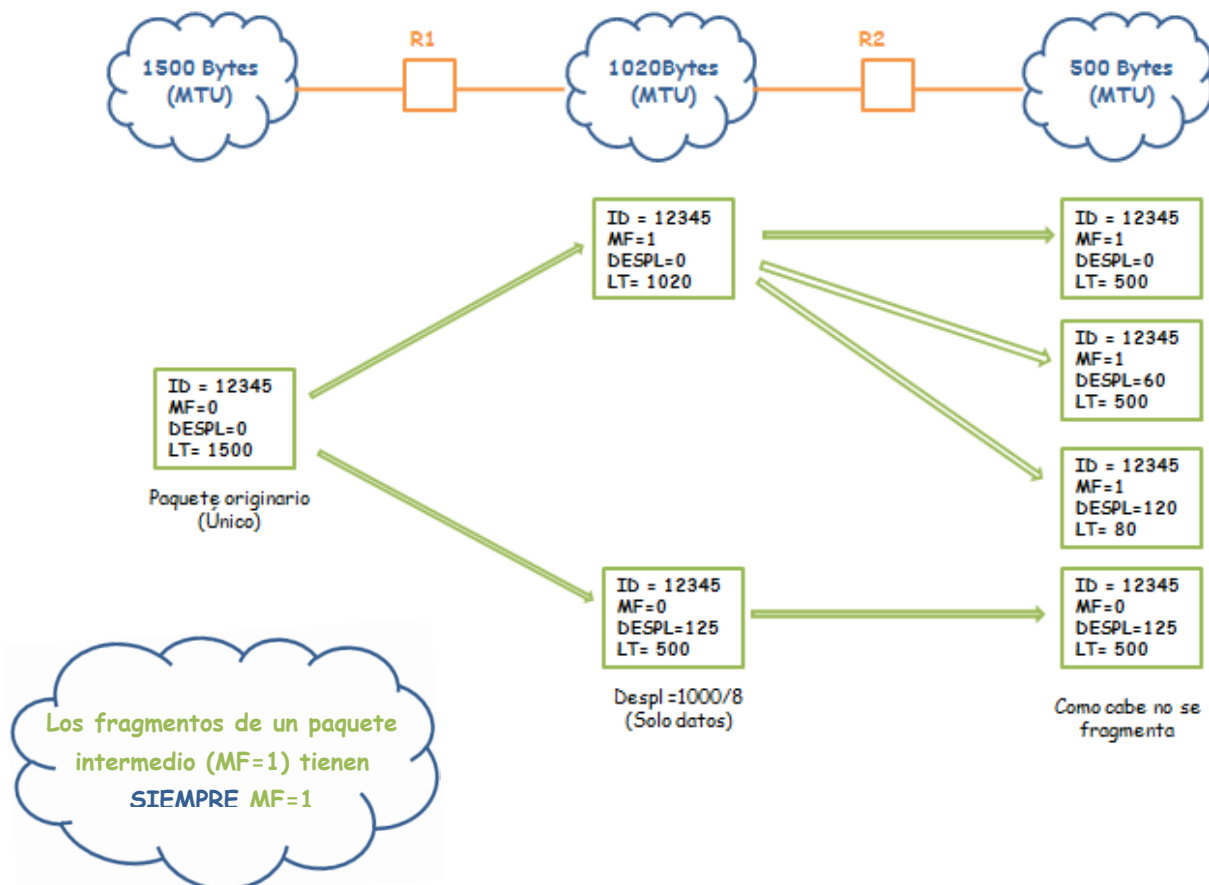
Cada fragmento implica replicar cabeceras, esto aumenta la carga de tráfico y proceso, ya que, estamos añadiendo redundancia.

Incrementa la probabilidad de perder un datagrama (paquete IP). Cuando se pierde un fragmento produce la pérdida del datagrama completo.

El router destino arranca un temporizador de reensamblado cuando recibe un primer fragmento. Si el temporizador finaliza y no han llegado todos los fragmentos se elimina el resto del datagrama.

Para evitar fragmentar se busca la MTU mínima y se mandan los paquetes con un tamaño menor que ese.

\* **EJEMPLO  $\Rightarrow$**



Cada fragmento es un mundo, los fragmentos de un mismo paquete no tienen por que encaminarse por el mismo camino.

• **DEFRAGMENTACION:**

\* El router destino comprueba el identificador del fragmento

\* Mira el desplazamiento y va rellenando huecos, cuando completa el paquete lo sube al nivel superior.

Un router intermedio no puede defragmentar porque:

1. Los routers son vagos, se necesitan buffers enormes para acumular los fragmentos hasta que llegue el último, si es que llega.
2. Nadie puede asegurar que el paquete pase por un router determinado, los fragmentos de un paquete son independientes.



## 9. PROTOCOLO ICMPv4.

Es el protocolo de envío de mensajes de control en Internet, para ello se utilizan mensajes ICMP.

El origen del mensaje ICMP es algún router o maquina destinataria del paquete.

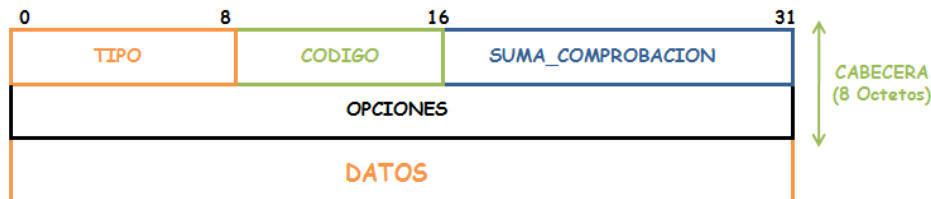
El destino del mensaje siempre va a ser la maquina origen, nunca un router o equipos intermedios.

El protocolo ICMP nunca hace fiable el nivel IP, porque incluso se pueden llegar a perder los mensajes ICMP.

### 9.1 MENSAJE ICMP.

Los mensajes ICMP se encapsulan dentro de un paquete IP, que a su vez se encapsulara dentro de la trama correspondiente para poder enviarlo.

#### • FORMATO:



- **TIPO:** Tipo de mensaje ICMP
- **CODIGO DEL ERROR:** Información adicional y específica sobre el tipo del mensaje ICMP.
- **SUMA DE COMPROBACIÓN:** Equivale a la longitud total de la cabecera IP. Se mide en octetos y representa Datos + Cabecera ICMP
- **OPCIONES:** Como máximo puede ocupar 4 octetos y se pueden usar o no.
- **DATOS:** Cabecera IP + 8 primeros octetos del campo de datos del paquete IP.

#### • TIPOS DE MENSAJES ICMP:

- **INFORME DE ERRORES:** Problemas que un router o la maquina destino puede encontrar al procesar un paquete IP.

##### 1. Destino Inalcanzable: Tipo =3

- \* Red/Puerto/Protocolo/Maquina destino no alcanzable.
- \* Fragmentación necesaria no realizada: paquete > MTU y DF=1
- \* Fallo de encaminamiento: el router no sabe por dónde encaminar el paquete
- \* Red destinataria / Maquina destinataria inalcanzable por el tipo de servicio.
- \* Comunicación con la red destinataria/ maquina destinataria prohibida por el administrador.

##### 2. Tiempo excedido: Tipo =11

- \* Vence el time to live del paquete que se envía (Código = 0)
- \* Tiempo de reensamblado excedido en la maquina destino (Código = 1).

##### 3. Problemas con los parámetros: Tipo =12. Campo opcional: Puntero (8 bits).

- \* Falla un parámetro (Código =0) ⇒ Puntero identifica el octeto que causo el problema.
- \* Falta un parámetro (Código =1) ⇒ Sin Puntero.

- **CONSULTA:** Ayudan a un sistema a tener información de otro sistema. (Código =0)

##### 1. Solicitud de ECO: Tipo 8

##### 2. Respuesta de ECO: Tipo 0

La combinación de ambos mensajes determina si dos sistemas se pueden comunicar entre sí, es decir, si hay comunicación IP. Si los mensajes ICMP se reciben es porque hay comunicación IP y los routers intermedios están encaminando.

El campo opción se compondrá por:

- \* Identificador (16 bits) ⇒ Numero para identificar a la solicitud y a su respuesta.



- \* Número de secuencia (16 bits)  $\Rightarrow$  Número para secuenciar más de una solicitud y respuesta en al mismo PING

El uso de mensajes ICMP de consulta permite:

- \* Saber si una maquina está viva y responde
- \* Calcular el tiempo aproximado (mínimo, máximo y promedio) de ida y vuelta de un paquete.
- \* Calcular la MTU mínima en el camino origen-destino: se comienza con la MTU de la red de acceso prohibiéndose fragmentar, y se va reduciendo hasta recibir un mensaje ICMP de destino inalcanzable por fragmentación necesaria y no realizada.

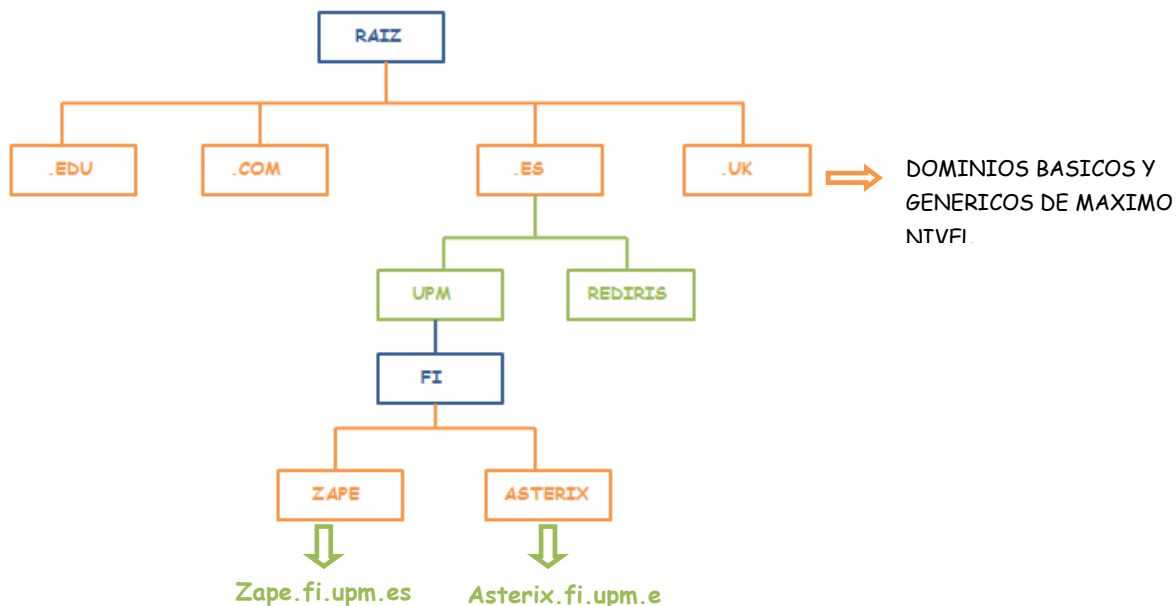
## 10. Dns.

- **DNS:** Jerarquía de nombres simbólicos de máquinas repartidas en un base de datos distribuida mediante servidores de nombres por toda Internet.

La base de datos se consulta por las aplicaciones de usuario para llevar a cabo la traducción entre nombres simbólicos u sus correspondientes direcciones numéricas.

Cada organización dispone de su propio servidor DNS. Ningún servidor de nombres contiene la base de datos completa, lo que hacen es comunicarse entre ellos vía TCP/IP, cuando alguno necesite resolver la dirección que le pertenezca.

Los dominios se ordenan de derecha a izquierda, del más general al más particular, separando cada nombre simbólico por un punto.



- **PROTOCOLO DNS:** Ofrece un servicio de traducción de una dirección simbólica en una dirección IP.

